基于攻防微分博弈的网络安全防御决策方法

张恒巍[1,2],李 涛[1],黄世锐[1]
(1. 信息工程大学三院,河南郑州 450001; 2. 信息保障技术重点实验室,北京 100093)

摘 要: 为准确分析快速变化和连续对抗的网络攻防行为,借鉴传染病动力学理论,提出安全状态演化模型分析网络系统安全状态的变化过程. 在此基础上,构建攻防微分博弈模型,设计鞍点策略的求解方法,并以此为依据给出最优防御策略选取算法,实现在动态连续攻防过程中的实时最优防御决策. 通过仿真实验验证了模型和算法的有效性,并在分析实验数据的基础上提出了针对性的网络防御建议.

关键词: 网络安全; 网络攻防; 安全状态演化; 博弈论; 微分博弈; 网络防御; 攻防行为分析; 最优策略选取
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)06-1428-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.06.023

Network Defense Decision-Making Method Based on Attack-Defense Differential Game

ZHANG Heng-wei[1,2], LI Tao[1], HUANG Shi-rui[1]
(1. *The Third Institute, Information Engineering University, Zhengzhou, Henan* 450001, *China*;
2. *Science and Technology on Information Assurance Laboratory, Beijing* 100093, *China*)

Abstract: To precisely analyze the quick status transformation and continuous confrontation in network, the security status transformation model is formulated to analyze the transformation of network security status, referring to the infectious disease dynamics. Based on the mentioned above, the attack-defense differential game model is formulated in the paper. Then saddle point strategies of the game model are figured out, through which the algorithm of optimal defense strategies selection in the consistent confrontation is given, which could help make optimal defense decision in dynamic and continuous attack-defense confrontation. Finally, the experimental results show model and method proposed in this paper are valid, and some instructive conclusions on network defense are drawn by the experimental analysis.

Key words: network security; network attack and defense; security status transformation; game theory; differential game; network defense; attack-defense analysis; optimal strategies selection

1 引言

网络基础设施已经成为信息时代社会有机运行的神经系统. 增强网络安全防御能力,确保网络空间安全已成为亟待解决的迫切问题[1]. 网络安全的本质在攻防对抗,博弈理论与网络攻防所具有的目标对立性、关系非合作性和策略依存性十分吻合[2]. 目前,运用博弈模型分析网络攻防行为,开展防御决策研究已经取得部分成果.

一方面,针对网络攻防中攻击者和防御者的行为信息与收益信息是否透明,可以分别采用完全信息静态博弈模型[3]以及非完全信息静态博弈模型[4]研究网络防御策略选取问题. 另一方面,由于攻防过程中攻击方和防御方的行动一般不具有同时性,构建动态网络攻防博弈模型[5,6]开展网络防御决策研究,具有更强的理论指导价值. 当进一步考虑攻防行为信息对博弈过程的影响时,可在引入信号博弈模型[7,8]的基础上,研究有限信息条件下的动态安全风险评估和防御决策.

考虑到攻防对抗具有多阶段、连续性的特征,因此将其视为多阶段博弈过程更加合理[9]. 文献[10]以WSN防御机制为背景,基于攻防重复博弈模型研究无线网络抗DDOS攻击的方法. 文献[11]基于不完全信息动态博弈理论,构建多阶段攻防信号博弈模型,研究了有限信息条件下多阶段攻防的防御策略选取问题.

目前,网络攻防向快速、实时、多样化的方向发展,上述基于传统动态博弈的分析方法已不能满足实际要求. 亟需建立能够分析动态、连续、实时攻防过程的博弈

收稿日期:2016-12-18;修回日期:2017-03-22;责任编辑:梅志强
基金项目:国家自然科学基金(No. 61303074, No. 61309013);信息保障技术重点实验室开放基金(No. KJ-15-110)

模型.微分博弈是时间实时变化情况下描述冲突对抗中连续控制过程的理论方法[12],能够更好地分析攻防双方的连续、实时对抗行为,实现最优防御策略动态选取.但是,攻防微分博弈模型的构建、求解和分析难度大,目前据我们所知尚未有公开文献予以讨论.

本文借鉴传染病动力学理论[13],构建了状态演化模型 NIRM 分析网络系统安全状态的变化过程.在此基础上,构建攻防微分博弈模型,提出描述策略选取和收益变化情况的攻防决策控制函数以及收益积分函数.通过对鞍点策略的求解和分析,得到最优策略控制轨迹的描述方程,并设计了最优防御策略实时选取算法.

2　攻防微分博弈模型

2.1　攻防过程中的安全状态演化分析

对于在大量节点构成的网络系统上发生的攻防对抗,一方面,组成系统的节点的安全状态不断迁移变化;另一方面,处于不同安全状态的节点的数量动态改变.为刻画这一过程,本文借鉴 SIR 模型并加以扩展,把网络系统中的节点类比为 SIR 模型中的个体,将 SIR 模型中的演化状态扩展为 4 个,构建安全状态演化模型 NIRM.

NIRM 模型包含四个状态:正常状态 N(Normal)、感染状态 I(Infected)、修复状态 R(Restored)、受损状态 M(Malfunctioned).

(1)N:网络节点处于正常工作状态,但是由于节点内在的脆弱性,节点可能遭受攻击;

(2)I:网络节点处于已被攻击策略渗透或传染的状态,但是还未出现服务质量下降,同时攻击者可以利用该节点攻击相邻节点;

(3)R:网络节点已被防御策略保护,对攻击策略具有免疫能力的状态;

(4)M:网络节点处于服务质量严重下降甚至丧失服务能力的状态.

网络节点在四种状态下的迁移如图 1 所示.

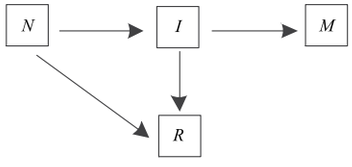

图1　NIRM模型中节点状态转换示意图

在 NIRM 模型中,节点状态有 4 种迁移路径.

$N\to I$:若防御策略失败,则正常节点被感染,此时破坏效果处于潜伏期,节点服务质量未遭受损失;但是,攻击者能够利用该节点攻击邻接节点.

$N\to R$:若防御策略成功,则正常节点具有对攻击的免疫能力.

$I\to R$:防御策略识别感染节点并清除感染,避免了感染节点的损失并将其转化为免疫状态.

$I\to M$:若防御策略失败,则破坏效果出现,感染节点丧失服务功能.

设网络节点总数为 Q,t 时刻处于四种状态的节点数量依次用变量 $N(t)$、$I(t)$、$R(t)$ 和 $M(t)$ 表示,则在 $\forall t\in[t_0,T]$,有 $N(t)+I(t)+R(t)+M(t)=Q$.

假设节点以密度 α 部署在网络系统中,则对某个网络节点而言,与其相连的节点数为 $\pi\alpha r^2$. r 表示两个节点的网络连接距离,当 $r=1$ 时,代表两个节点直接相连.对于一个感染节点,能与其直接通信的相邻节点的数量为 $\pi\alpha$.在 t 时刻,处于正常状态的节点在全部节点中所占的比例是 $N(t)/Q$.因此,t 时刻和感染节点相邻的正常节点的数量为 $\pi\alpha I(t)N(t)/Q$.

攻击和防御策略的对抗结果是决定状态迁移的关键因素.通过一个攻防实例具体说明,依据攻击强度将攻击策略分为强、中、弱三类,依次表示为 A_H、A_M、A_L,平均攻击强度可以依次表示为$\overline{e_A^H},\overline{e_A^M},\overline{e_A^L}\in[0,1]$.攻击者在时刻 t 采用混合策略 $P_A(t)=(p_A^H(t),p_A^M(t),p_A^L(t))$,则攻击期望效用为 $a(t)=p_A^H(t)\overline{e_A^H}+p_A^M(t)\overline{e_A^M}+p_A^L(t)\overline{e_A^L}$,简记为 a.

同理,依据防御强度将防御策略分为 D_H、D_L,其平均防御强度依次为$\overline{e_D^H},\overline{e_D^L}\in[0,1]$,防御者在时刻 t 采用混合策略 $P_D(t)$,则防御期望效用表示为 $d(t)=p_D^H(t)\overline{e_D^H}+p_D^L(t)\overline{e_D^L}$,简记为 d.通过攻防效用差值表示攻击是否成功,记作 $\eta(t)=a(t)-d(t)$,并且$|\eta(t)|\in[0,1]$.当 $\eta(t)>0$ 时,表示攻击成功;否则,表示攻击失败.

利用攻防效用 $\eta(t)$ 分析迁移路径,可得描述状态迁移可能性的迁移参数 η_{NI}、η_{NR}、η_{IR}、η_{IM}.

$$\eta_{NI}=\begin{cases}0, & \eta(t)\leqslant 0\\ \eta(t), & \eta(t)>0\end{cases};\quad \eta_{NR}=\begin{cases}|\eta(t)|, & \eta(t)\leqslant 0\\ 0, & \eta(t)>0\end{cases}$$

$$\eta_{IR}=\begin{cases}|\eta(t)|, & \eta(t)\leqslant 0\\ 0, & \eta(t)>0\end{cases};\quad \eta_{IM}=\begin{cases}0, & \eta(t)\leqslant 0\\ \eta(t), & \eta(t)>0\end{cases}$$

综上,得到描述网络节点安全状态变化的微分方程组.

$$\begin{cases}\dot{N}=-\eta_{NI}(t)\alpha\pi I(t)N(t)/Q-\eta_{NR}(t)N(t)\\ \dot{I}=\eta_{NI}(t)\alpha\pi I(t)N(t)/Q-\eta_{IM}(t)I(t)-\eta_{IR}(t)I(t)\\ \dot{R}=\eta_{NR}(t)N(t)+\eta_{IR}(t)I(t)\\ \dot{M}=\eta_{IM}(t)I(t)\\ \forall t\in[t_0,T],N(t)+I(t)+R(t)+M(t)=Q\end{cases}\tag{1}$$

2.2　攻防微分博弈模型定义

定义 1　网络攻防微分博弈模型 ADDG(Attack-Defense Differential Game)可以表示为 ADDG=(N,Θ,B,t,

x,S,f,U).

(1) $N=(N_D,N_A)$是攻防博弈的参与人集合. N_D 代表防御者,N_A 代表攻击者.

(2) $\Theta=(\Theta_D,\Theta_A)$是防御者与攻击者的类型空间,$\Theta_D=\{D_i\mid i=1,2,\cdots,n\}$,$\Theta_A=\{A_j\mid j=1,2,\cdots,m\}$.

(3) $B=(DS,AS)$是动作空间. $AS=(\delta_1,\cdots,\delta_g)$和 $DS=(\beta_1,\cdots,\beta_k)$表示攻防动作集合,$g,k\geqslant 1$.

(4) t 代表网络攻防过程中的时刻,$t\in[t_0,T]$.

(5) $x(t)=(N(t),I(t),R(t),M(t))$是网络系统的状态变量.

(6) $S=(D(t),A(t))$代表 t 时刻的控制策略. $D(t)=\{P_D(t)\mid P_D(t)=(p_D^i(t)),1\leqslant i\leqslant n\}$代表防御者在 t 时刻选取的混合策略,$\sum_{i=1}^{n}p_D^i(t)=1$;同理 $A(t)=\{P_A(t)\mid P_A(t)=(p_A^j(t)),1\leqslant j\leqslant m\}$代表攻击者在 t 时刻的混合策略,$\sum_{j=1}^{m}p_A^j(t)=1$. 控制策略是当前时刻 t、初始状态 $x(t_0)$和当前状态 $x(t)$的函数,即 $P_A(t)=P_A(t,x(t_0),x(t))$,$P_D(t)=P_D(t,x(t_0),x(t))$.

(7) $f=\{f_N,f_I,f_R,f_M\}$是状态迁移函数. 其中,$f_N=\frac{dN(t)}{dt}=\dot{N}$,$f_I=\frac{dI(t)}{dt}=\dot{I}$,$f_R=\frac{dR(t)}{dt}=\dot{R}$,$f_M=\frac{dM(t)}{dt}=\dot{M}$. 状态迁移的分析参见 2.1 节.

(8) $U=(U_D,U_A)$是攻防双方收益函数的集合. $U=\int_{t_0}^{T}g(t,x(t),P_A(t),P_D(t))dt$ 是随时间动态变化的积分函数.

当正常节点转变为感染节点时,设回报系数为 r_1;当感染节点或正常节点转变为修复节点时,设回报系数为 r_2;当感染节点转变为受损节点时,设回报系数为 r_3. 本文采用统计平均值定义回报系数 $r_1,r_2,r_3\in[0,10]$.

根据上述分析,可得 t 时刻的防御回报 $r_D(t)$和攻击回报 $r_A(t)$.

$$\begin{aligned}r_D(t)=&r_2[\eta_{NR}(t)N(t)+\eta_{IR}(t)I(t)]\\&-r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q]-r_3[\eta_{IM}(t)I(t)]\end{aligned}\tag{2}$$

$$\begin{aligned}r_A(t)=&r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q]+r_3[\eta_{IM}(t)I(t)]\\&-r_2[\eta_{NR}(t)N(t)+\eta_{IR}(t)I(t)]\end{aligned}\tag{3}$$

攻防双方执行策略时均会消耗相应的策略代价,策略代价一般正比于策略效能,参考文献[10]的成本度量方法,设 t 时刻的策略执行代价为

$$\begin{aligned}v_D&=\frac{d^2}{2}c_D(N(t)+I(t)+R(t)+M(t))\\v_A&=\frac{a^2}{2}c_A(N(t)+I(t)+R(t)+M(t))\end{aligned}\tag{4}$$

c_D、c_A 为防御和攻击策略的成本/效用系数,c_D、$c_A\in[1,10]$. 综合考虑策略的回报和执行代价,可得攻防双方的收益函数.

$$\begin{aligned}U_D(P_A(t),P_D(t))=&\int_{t_0}^{T}\Big\{r_2[\eta_{NR}(t)N(t)+\eta_{IR}(t)I(t)]\\&-r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q]-r_3[\eta_{IM}(t)I(t)]\\&-\frac{c_D}{2}d^2[N(t)+I(t)+R(t)+M(t)]\Big\}dt\end{aligned}\tag{5}$$

$$\begin{aligned}U_A(P_A(t),P_D(t))=&\int_{t_0}^{T}\Big\{r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q]\\&-r_2[\eta_{NR}(t)N(t)+\eta_{IR}(t)I(t)]+r_3[\eta_{IM}(t)I(t)]\\&-\frac{c_A}{2}a^2[N(t)+I(t)+R(t)+M(t)]\Big\}dt\end{aligned}\tag{6}$$

3 最优防御策略选取

3.1 鞍点策略求解

博弈均衡下攻防最优策略组成的策略对$(P_A^*(t),P_D^*(t))$,称为攻防微分博弈的鞍点策略.

定义 2 鞍点策略. 如果存在策略组合$(P_A^*(t),P_D^*(t))$,满足

$$\begin{cases}\forall P_A(t),U_A(P_A(t)^*,P_D(t)^*)\geqslant U_A(P_A(t),P_D(t)^*)\\\forall P_D(t),U_D(P_A(t)^*,P_D(t)^*)\geqslant U_D(P_A(t)^*,P_D(t))\end{cases}$$

则$(P_A^*(t),P_D^*(t))$称为攻防微分博弈的鞍点,也称为攻防双方的鞍点策略,简称鞍点策略.

定理 1 如果存在共态函数 $K_i(t):[t_0,T]\times\mathcal{R}^k\to\mathcal{R}$,$i\in(D,A)$,使得下列条件成立,则存在鞍点策略$(P_A^*(t),P_D^*(t))$.

$$\begin{cases}P_A^*(t)=\underset{P_A(t)}{\operatorname{argmax}}\{f(t,x^*(t),P_A(t),P_D^*(t))K_A(t)\\\qquad\qquad+g(t,x^*(t),P_A(t),P_D^*(t))\}\\P_D^*(t)=\underset{P_D(t)}{\operatorname{argmax}}\{f(t,x^*(t),P_A^*(t),P_D(t))K_D(t)\\\qquad\qquad+g(t,x^*(t),P_A^*(t),P_D(t))\}\end{cases}\tag{7}$$

$$\begin{cases}\frac{d}{dt}x^*(t)=f(t,x^*(t),P_A^*(t),P_D^*(t))\\x^*(t_0)=x(t_0)\end{cases}\tag{8}$$

$$\begin{cases}\frac{d}{dt}K_A(t)=-\frac{\partial}{\partial x^*}\{f(t,x^*(t),P_A^*(t),P_D^*(t))K_A(t)\\\qquad\qquad+g(t,x^*(t),P_A^*(t),P_D^*(t))\}\\\frac{d}{dt}K_D(t)=-\frac{\partial}{\partial x^*}\{f(t,x^*(t),P_A^*(t),P_D^*(t))K_D(t)\\\qquad\qquad+g(t,x^*(t),P_A^*(t),P_D^*(t))\}\end{cases}\tag{9}$$

证明 根据最优控制理论中的庞特里亚金最大值定理[14],可以证明共态函数 $K_i(t)$的存在性. 而且当 $t\in[t_0,T]$时,$t\to H(t,K_i(t),x^*,P_A^*(t),P_D^*(t))$为常数. 因

此,定理 1 得证,攻防微分博弈存在鞍点策略.

基于以上证明思路,提出求解鞍点策略的过程和步骤,构造如下 Hamilton 函数

$$\begin{aligned}
&H(t,K_{\mathrm{D}}(t),x,P_{\mathrm{A}}(t),P_{\mathrm{D}}(t))\\
&=g(t,x,P_{\mathrm{A}}(t),P_{\mathrm{D}}(t))\\
&\quad+\sum_{x\in\{N,I,R,M\}}K_{\mathrm{D}}^{x}(t)f((t,x,P_{\mathrm{A}}(t),P_{\mathrm{D}}(t))\\
&=r_2[\eta_{NR}(t)N(t)+\eta_{IR}(t)I(t)]\\
&\quad-r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q]-r_3[\eta_{IM}(t)I(t)]\\
&\quad-\frac{d^2}{2}c_{\mathrm{D}}(N(t)+I(t)+R(t)+M(t))\\
&\quad-K_{\mathrm{D}}^{N}(t)[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q+\eta_{NR}(t)N(t)]\\
&\quad+K_{\mathrm{D}}^{I}(t)[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q\\
&\quad-\eta_{IM}(t)I(t)-\eta_{IR}(t)I(t)]+K_{\mathrm{D}}^{R}(t)[\eta_{NR}(t)N(t)\\
&\quad+\eta_{IR}(t)I(t)]+K_{\mathrm{D}}^{M}(t)\eta_{IM}(t)I(t)\\
&=\eta_{NI}(t)\cdot\alpha\pi I(t)N(t)/[Q(K_{\mathrm{D}}^{I}(t)]-K_{\mathrm{D}}^{N}(t)-r_1)\\
&\quad+\eta_{NR}(t)\cdot N(t)(K_{\mathrm{D}}^{R}(t)-K_{\mathrm{D}}^{N}(t)+r_2)\\
&\quad+\eta_{IR}(t)\cdot I(t)(K_{\mathrm{D}}^{R}(t)-K_{\mathrm{D}}^{I}(t)+r_2)\\
&\quad+\eta_{IM}(t)\cdot I(t)(K_{\mathrm{D}}^{M}(t)-K_{\mathrm{D}}^{I}(t)-r_3)\\
&\quad-\frac{d^2}{2}c_{\mathrm{D}}(N(t)+I(t)+R(t)+M(t))
\end{aligned}\tag{10}$$

计算上述 Hamilton 函数中的共态函数 $K_{\mathrm{D}}(t)$.

对于 $x\in\{N(t),I(t),R(t),M(t)\}$,可以得到

$$K_{\mathrm{D}}(t)=(K_{\mathrm{D}}^{x}(t))^{\mathrm{T}}=(K_{\mathrm{D}}^{N}(t),K_{\mathrm{D}}^{I}(t),K_{\mathrm{D}}^{R}(t),K_{\mathrm{D}}^{M}(t))^{\mathrm{T}}.$$

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}t}K_{\mathrm{D}}^{N}(t)&=-\frac{\partial}{\partial N(t)}H(t,K_{\mathrm{D}}(t),x^*,P_{\mathrm{A}}^*(t),P_{\mathrm{D}}^*(t))\\
&=[r_1\eta_{NI}^*(t)\alpha\pi I^*(t)/Q-r_2\eta_{NR}^*(t)]\\
&\quad+K_{\mathrm{D}}^{N}(t)[\eta_{NI}^*(t)\alpha\pi I^*(t)/Q+\eta_{NR}(t)]\\
&\quad-K_{\mathrm{D}}^{I}(t)\eta_{NI}^*(t)\alpha\pi I^*(t)/Q-K_{\mathrm{D}}^{R}(t)\eta_{NR}^*(t)\\
&\quad+\frac{c_{\mathrm{D}}}{2}d^2
\end{aligned}\tag{11}$$

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}t}K_{\mathrm{D}}^{I}(t)&=-\frac{\partial}{\partial I(t)}H(t,K_{\mathrm{D}}(t),x^*,P_{\mathrm{A}}^*(t),P_{\mathrm{D}}^*(t))\\
&=-r_2\eta_{IR}^*(t)+r_1\eta_{NI}^*(t)\alpha\pi N^*(t)/Q\\
&\quad+r_3\eta_{IM}^*(t)+K_{\mathrm{D}}^{N}(t)[\eta_{NI}^*(t)\alpha\pi N^*(t)/Q]\\
&\quad-K_{\mathrm{D}}^{I}(t)[\eta_{NI}^*(t)\alpha\pi N^*(t)/Q-\eta_{IM}^*(t)-\eta_{IR}^*(t)]\\
&\quad-K_{\mathrm{D}}^{R}(t)\eta_{IR}^*(t)-K_{\mathrm{D}}^{M}(t)\eta_{IM}^*(t)+\frac{c_{\mathrm{D}}}{2}d^2
\end{aligned}\tag{12}$$

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}t}K_{\mathrm{D}}^{R}(t)&=-\frac{\partial}{\partial R(t)}H(t,K_{\mathrm{D}}(t),x^*,P_{\mathrm{A}}^*(t),P_{\mathrm{D}}^*(t))\\
&=\frac{c_{\mathrm{D}}}{2}d^2
\end{aligned}\tag{13}$$

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}t}K_{\mathrm{D}}^{M}(t)&=-\frac{\partial}{\partial M(t)}H(t,K_{\mathrm{D}}(t),x^*,P_{\mathrm{A}}^*(t),P_{\mathrm{D}}^*(t))\\
&=\frac{c_{\mathrm{D}}}{2}d^2
\end{aligned}\tag{14}$$

同理,对于攻击者可以得到共态函数 $K_{\mathrm{A}}^{N}(t)$,$K_{\mathrm{A}}^{I}(t)$,$K_{\mathrm{A}}^{R}(t)$,$K_{\mathrm{A}}^{M}(t)$. 为方便后续阐述,很据式(11)~(14)构造辅助表达式.

$$\begin{aligned}
&\frac{\mathrm{d}K_{\mathrm{D}}^{N}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{N}(t),\quad\frac{\mathrm{d}K_{\mathrm{D}}^{I}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{I}(t)\\
&\frac{\mathrm{d}K_{\mathrm{D}}^{R}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{R}(t),\quad\frac{\mathrm{d}K_{\mathrm{D}}^{M}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{M}(t)
\end{aligned}\tag{15}$$

$$\begin{aligned}
&\frac{\mathrm{d}K_{\mathrm{A}}^{N}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{N}(t),\quad\frac{\mathrm{d}K_{\mathrm{A}}^{I}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{I}(t)\\
&\frac{\mathrm{d}K_{\mathrm{A}}^{R}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{R}(t),\quad\frac{\mathrm{d}K_{\mathrm{A}}^{R}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{R}(t)
\end{aligned}\tag{16}$$

在计算共态函数的基础上,采用动态规划方法求解鞍点策略. 为方便说明和理解,以 2.1 节的攻防实例进行具体分析.

首先,计算如下动态规划问题.

$$\begin{aligned}
&\forall P_{\mathrm{A}}(t),P_{\mathrm{D}}(t),t\in[t_0,T],x\in\{N(t),I(t),R(t),M(t)\}\\
&\begin{cases}
H(t,K_{\mathrm{D}}(t),x^*,P_{\mathrm{A}}^*,P_{\mathrm{D}}^*)\geqslant H(t,K_{\mathrm{D}}(t),x^*,P_{\mathrm{A}}^*,P_{\mathrm{D}})\\
H(t,K_{\mathrm{A}}(t),x^*,P_{\mathrm{A}}^*,P_{\mathrm{D}}^*)\geqslant H(t,K_{\mathrm{A}}(t),x^*,P_{\mathrm{A}},P_{\mathrm{D}}^*)\\
\dfrac{\mathrm{d}K_{\mathrm{D}}^{N}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{N}(t),\dfrac{\mathrm{d}K_{\mathrm{D}}^{I}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{I}(t)\\
\dfrac{\mathrm{d}K_{\mathrm{D}}^{R}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{R}(t),\dfrac{\mathrm{d}K_{\mathrm{D}}^{M}(t)}{\mathrm{d}t}=\lambda_{\mathrm{D}}^{M}(t)\\
\dfrac{\mathrm{d}K_{\mathrm{A}}^{N}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{N}(t),\dfrac{\mathrm{d}K_{\mathrm{A}}^{I}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{I}(t)\\
\dfrac{\mathrm{d}K_{\mathrm{A}}^{R}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{R}(t),\dfrac{\mathrm{d}K_{\mathrm{A}}^{M}(t)}{\mathrm{d}t}=\lambda_{\mathrm{A}}^{M}(t)\\
\dfrac{\mathrm{d}N^*(t)}{\mathrm{d}t}=-\eta_{NI}^*(t)\alpha\pi I^*(t)N^*(t)/Q-\eta_{NR}(t)N^*(t)\\
\dfrac{\mathrm{d}R^*(t)}{\mathrm{d}t}=\eta_{NR}^*(t)N^*(t)+\eta_{IR}^*(t)I^*(t)\\
\dfrac{\mathrm{d}I^*(t)}{\mathrm{d}t}=\eta_{NI}^*(t)\alpha\pi I^*(t)N^*(t)/Q\\
\qquad\qquad-I^*(t)(\eta_{IM}^*(t)+\eta_{IR}^*(t))\\
\dfrac{\mathrm{d}M^*(t)}{\mathrm{d}t}=\eta_{IM}^*(t)I^*(t)\\
N^*(t_0)=N(t_0),I^*(t_0)=I(t_0)\\
R^*(t_0)=R(t_0),M^*(t_0)=M(t_0)
\end{cases}
\end{aligned}\tag{17}$$

得到 $K_{\mathrm{D}}^{N}(t)$、$K_{\mathrm{D}}^{I}(t)$、$K_{\mathrm{D}}^{R}(t)$、$K_{\mathrm{D}}^{M}(t)$ 以及 $N^*(t)$、$I^*(t)$、$R^*(t)$、$M^*(t)$.

然后,令 $\dfrac{\partial H^*}{\partial p_{\mathrm{D}}^{H}(t)}=0$,则可以计算得到 $P_{\mathrm{D}}^*(t)=(p_{\mathrm{D}}^{H}(t)^*,p_{\mathrm{D}}^{L}(t)^*)$.

当 $\eta(t)\leqslant 0$ 时;

$$\begin{aligned}
p_{\mathrm{D}}^{H}(t)^*=\{&[r_2+K_{\mathrm{D}}^{R}(t)-K_{\mathrm{D}}^{N}(t)]N^*(t)+[r_2+K_{\mathrm{D}}^{R}(t)\\
&-K_{\mathrm{D}}^{I}(t)]I^*(t)-\overline{e_{\mathrm{D}}^{L}}c_{\mathrm{D}}Q\}/[(\overline{e_{\mathrm{D}}^{H}}-\overline{e_{\mathrm{D}}^{L}})c_{\mathrm{D}}Q]
\end{aligned}\tag{18}$$

当 $\eta(t)>0$ 时；

$$p_{\mathrm{D}}^{H}(t)^{*}=\{[r_1+K_{\mathrm{D}}^{N}(t)-K_{\mathrm{D}}^{I}(t)]\alpha\pi I^{*}(t)N^{*}(t)/Q+[r_3+K_{\mathrm{D}}^{I}(t)-K_{\mathrm{D}}^{M}(t)]I^{*}(t)-\overline{e_{\mathrm{D}}^{L}}c_{\mathrm{D}}Q\}/[(\overline{e_{\mathrm{D}}^{H}}-\overline{e_{\mathrm{D}}^{L}})c_{\mathrm{D}}Q] \tag{19}$$

并且总有

$$p_{\mathrm{D}}^{L}(t)^{*}=1-p_{\mathrm{D}}^{H}(t)^{*} \tag{20}$$

同理，令 $\frac{\partial H^{*}}{\partial p_{\mathrm{A}}^{H}(t)}=0$，$\frac{\partial H^{*}}{\partial p_{\mathrm{A}}^{M}(t)}=0$，计算得到 $P_{\mathrm{A}}^{*}(t)=(p_{\mathrm{A}}^{H}(t)^{*},p_{\mathrm{A}}^{M}(t)^{*},p_{\mathrm{A}}^{L}(t)^{*})$.

当 $\eta(t)\leqslant 0$ 时；

$$p_{\mathrm{A}}^{H}(t)^{*}=\{[r_2+K_{\mathrm{A}}^{N}(t)-K_{\mathrm{A}}^{R}(t)]N^{*}(t)+[r_2+K_{\mathrm{A}}^{I}(t)-K_{\mathrm{A}}^{R}(t)]I^{*}(t)-\overline{e_{\mathrm{A}}^{L}}c_{\mathrm{A}}Q\}/[(\overline{e_{\mathrm{A}}^{H}}-\overline{e_{\mathrm{A}}^{L}})c_{\mathrm{A}}Q] \tag{21}$$

$$p_{\mathrm{A}}^{M}(t)^{*}=\{[r_2+K_{\mathrm{A}}^{N}(t)-K_{\mathrm{A}}^{R}(t)]N^{*}(t)+[r_2+K_{\mathrm{A}}^{I}(t)-K_{\mathrm{A}}^{R}(t)]I^{*}(t)-\overline{e_{\mathrm{A}}^{L}}c_{\mathrm{A}}Q\}/[(\overline{e_{\mathrm{A}}^{M}}-\overline{e_{\mathrm{A}}^{L}})c_{\mathrm{A}}Q] \tag{22}$$

当 $\eta(t)>0$ 时；

$$p_{\mathrm{A}}^{H}(t)^{*}=\{[r_1+K_{\mathrm{A}}^{I}(t)-K_{\mathrm{A}}^{N}(t)]\alpha\pi I(t)N^{*}(t)/Q+[r_3+K_{\mathrm{A}}^{M}(t)-K_{\mathrm{A}}^{I}(t)]I^{*}(t)-\overline{e_{\mathrm{A}}^{L}}c_{\mathrm{A}}Q\}/[(\overline{e_{\mathrm{A}}^{H}}-\overline{e_{\mathrm{A}}^{L}})c_{\mathrm{A}}Q] \tag{23}$$

$$p_{\mathrm{A}}^{M}(t)^{*}=\{[r_1+K_{\mathrm{A}}^{I}(t)-K_{\mathrm{A}}^{N}(t)]\alpha\pi I^{*}(t)N^{*}(t)/Q+[r_3+K_{\mathrm{A}}^{M}(t)-K_{\mathrm{A}}^{I}(t)]I^{*}(t)-\overline{e_{\mathrm{A}}^{L}}c_{\mathrm{A}}Q\}/[(\overline{e_{\mathrm{A}}^{M}}-\overline{e_{\mathrm{A}}^{L}})c_{\mathrm{A}}Q] \tag{24}$$

并且总有

$$p_{\mathrm{A}}^{L}(t)^{*}=1-p_{\mathrm{A}}^{H}(t)^{*}-p_{\mathrm{A}}^{M}(t)^{*} \tag{25}$$

3.2 最优防御策略选取算法及对比分析

将本文提出的方法和其它文献进行对比，结果见表 1.

算法 1 攻防微分博弈的最优防御策略选取算法

输入：攻防微分博弈模型

输出：最优防御策略 $P_{\mathrm{D}}^{*}(t)$

BEGIN

1. 初始化 ADDG = (N,Θ,B,t,x,S,f,U)；
2. 构建防御者类型空间 Θ_{D} 和攻击者类型空间 Θ_{A}；
3. 构建攻防行为空间 AS = $(\delta_1,\delta_2,\cdots,\delta_g)$ 和 DS = $(\beta_1,\beta_2,\cdots,\beta_k)$；
4. 根据式(1)构建状态演化微分方程组 $\dot{x}(t)=\{f_N,f_I,f_R,f_M\}$；
5. 初始化常量系数 $r_1,r_2,r_3,c_{\mathrm{D}},c_{\mathrm{A}}$；
6. 构造 Hamilton 函数 $H(t,K_{\mathrm{D}}(t),x,P_{\mathrm{A}}(t),P_{\mathrm{D}}(t))$ 和 $H(t,K_{\mathrm{A}}(t),x,P_{\mathrm{A}}(t),P_{\mathrm{D}}(t))$；
7. 根据式(11)～(14)，对于 $x\in\{N(t),I(t),R(t),M(t)\}$，计算 $K_{\mathrm{D}}(t)=(K_{\mathrm{D}}^{x}(t))^{\mathrm{T}}$；
8. 同理计算 $K_{\mathrm{A}}(t)=(K_{\mathrm{A}}^{x}(t))^{\mathrm{T}}$；
9. 利用动态规划方法计算方程(17)，求解 $K_{\mathrm{D}}(t)$、$K_{\mathrm{A}}(t)$ 和 $(N^{*}(t),I^{*}(t),R^{*}(t),M^{*}(t))$；
10. 对于防御者，由 $\frac{\partial H^{*}}{\partial p_{\mathrm{D}}^{i}(t)}=0$，计算 $p_{\mathrm{D}}^{i}(t)^{*}$，$1\leqslant i\leqslant n$；
11. 对于攻击者，由 $\frac{\partial H^{*}}{\partial p_{\mathrm{A}}^{j}(t)}=0$，计算 $p_{\mathrm{A}}^{j}(t)^{*}$，$1\leqslant j\leqslant m$；
12. Return $P_{\mathrm{D}}(t)=\{p_{\mathrm{D}}^{i}(t)^{*}\mid 1\leqslant i\leqslant n\}$；

END

表 1 对比分析表

文献	博弈类型	博弈者类型	攻防过程	决策时效性	模型通用性	均衡求解	具体应用
文献[4]	不完全信息静态	1	–	未考虑	差	详细	策略选取
文献[5]	不完全信息动态	2	单阶段	未考虑	差	无	效能评估
文献[6]	不完全信息动态	2	单阶段	未考虑	差	简单	机制分析
文献[11]	不完全信息动态	n	离散多阶段	未考虑	较好	详细	策略选取
本文	微分博弈	n	时间连续	好	较好	详细	策略选取

博弈者类型是指博弈模型中攻防双方是否区分不同类型以及类型的多少. 决策时效性是指选取的最优策略的有效时间. 如果只考虑一次性对抗过程，可视为单阶段攻防，所得最优策略也只适用于单阶段；如将对抗过程视为动态多阶段，则所得最优策略序列是离散的各个阶段中的最优策略. 本文基于微分博弈模型将时间因素引入攻防对抗分析，可以实现任意时刻的最优策略选取，相比其它文献具有更好的决策时效性. 模型的通用性是指模型中的类型集合和策略集合是否可以扩展. 均衡求解是指文献中是否给出均衡解的计算过程.

4 仿真实验及分析

4.1 实验环境描述

参考文献[6,10]和美国 MIT 的攻防行为数据库[15]，给出攻击和防御动作信息，如表 2 和表 3 所示. 采用仿真工具 Scalable Simulation Framework on Network (SSFNet)[16] 开展实验，参考文献[17]，在仿真实验中设置节点数量 $Q=1000$.

表 2　攻击动作描述

序号	攻击动作名称	攻击强度	攻击类型	平均强度
1	Remote buffer overflow	0.95		
2	Install Trojan	0.8	A_H	0.82
3	Steal account and crack it	0.7		
4	Send abnormal data to GIOP	0.5		
5	LPC to LSASS	0.4	A_M	0.45
6	Shutdown Database server	0.45		
7	Oracle TNS Listener	0.35		
8	Ftp rhost attack	0.3	A_L	0.3
9	Sr-Hard blood	0.25		

表 3　防御动作描述

序号	防御动作名称	防御强度	防御类型	平均强度
1	Limit packets from ports	0.8		
2	Install Oracle patch	0.8	D_H	
3	Reinstall Listener program	0.8		
4	Uninstall delete Trojan	0.7		0.71
5	Limit access to MDSYS. SDO _ CS	0.7		
6	Renew root data	0.6		
7	Restart Database server	0.6		
8	Limit SYN/ICMP packets	0.5		
9	Add physical resource	0.5		
10	Repair database	0.4		
11	Correct homepage	0.4	D_L	0.34
12	Delete suspicious account	0.3		
13	Redeploy firewall rule and filtrate malicious packets	0.3		
14	Patch SSH on Ftp	0.2		

4.2　实验分析

设常量参数 $r_1=2, r_2=4, r_3=9, c_D=5, c_A=4.3$. 其中,$r_1$、$r_2$、$r_3$ 为回报系数,根据网络拓扑以及节点分布情况和服务价值,采用统计平均值设定;c_D、c_A 为策略的成本/效用系数,根据表 2 和表 3 的数据采用算术平均值设定. 攻防对抗过程持续时间为 10m,即 $t\in[0,10]$. 利用 Matlab 2014 工具实现最优防御策略选取算法,得到攻防双方最优策略轨迹如图 2 ~ 图 4 所示.

(1)如图 2 所示,在 $t=0$ 时,$p_A^H(0)^*=0.72$,采用较高的概率选取强攻击策略 A_H. 此后 $p_A^H(t)^*$ 开始快速降低,在 $t=0.6$ 时刻后,$p_A^H(t)^*<0.5$. 从 $t=3$ 开始,$p_A^H(t)^*$ 趋近 0.09. 攻击者在 $t\in[0,0.6]$ 内以较高概率采用强攻击策略 A_H,目的是在短时间内实施“闪电战”,尽量扩大感染节点的数量,以及尽量使感染节点转变为受损状态,加大系统性能的实时损失和预期损失. 由于 A_H 的执行代价高,因此攻击者采用该策略在短时间内达到目标后,便减少使用概率以保证较高的费效比. 从 $t=3$ 时刻以后,A_H 的概率维持在 $p_A^H(t)^*=0.09$.

(2)如图 3 所示,在 $t\in[0,3]$ 内,攻击者采用策略 A_M 的概率虽在增加,但仍维持在非常低的水平 $p_A^M(t)^*<0.1$;$t=6$ 时刻以后,提高到 $p_A^M(t)^*>0.2$;$t=10$ 时刻,最终增加到 $p_A^M(t)^*=0.53$. 考虑策略实施代价,攻击者要想在攻防对抗全过程中取得优势,势必会加强对策略 A_M 的使用,以期取得较好的攻击效果和费效比.

(3)如图 4 所示,在 $t=0$ 时,$p_A^L(t)^*=0.28$,采用较低的概率选取策略 A_L. 在 $t\in[0,3]$ 内,$p_A^L(t)^*$ 迅速增

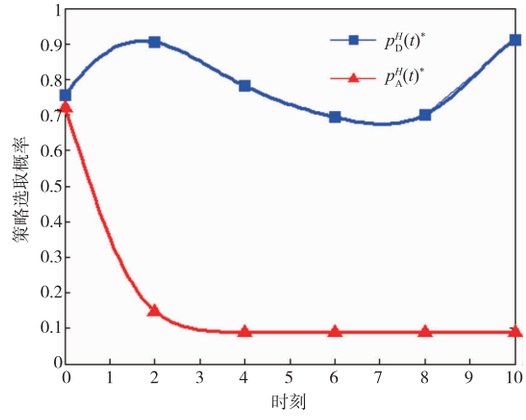

图2　$p_D^H(t)^*$和$p_A^H(t)^*$的最优控制轨迹

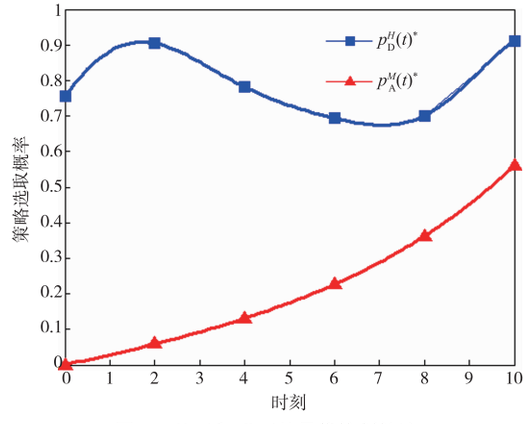

图3　$p_A^M(t)^*$和$p_D^H(t)^*$的最优控制轨迹

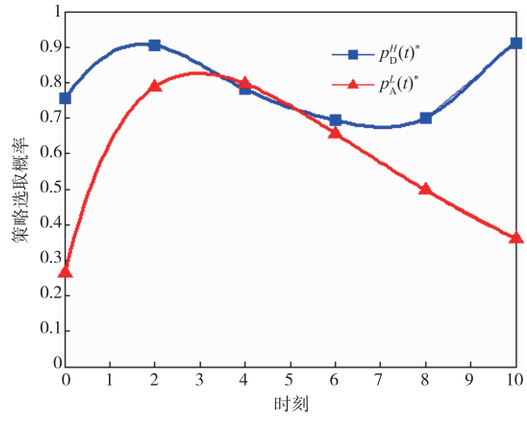

图4　$p_A^L(t)^*$和$p_D^H(t)^*$的最优控制轨迹

加,在 $t=3$ 时刻达到峰值 $p_A^L(t)^*=0.81$. 此后逐渐减少,在 $t=10$ 时刻,$p_A^L(t)^*=0.38$. 由于攻击者具有先发优势,往往采用高强度攻击进行突然袭击,力争最大化攻击效果. 因此,在 $t\in[0,0.6]$,$p_A^H(t)^* \gg p_A^L(t)^*$ 且 $p_A^H(t)^*>0.5$. 但是突袭效应能够持续的时间很短,当防御者察觉并调整防御措施后,采取高强度攻击的效果将显著下降,考虑到策略实施代价,将出现 $p_A^H(t)^*$ 迅速下降而 $p_A^L(t)^*$ 迅速上升的趋势. 随后,在 $t\in[3,10]$ 内,网络攻防进入相持阶段,攻击者趋向采用强度和代价均相对较低的策略,此时 $p_A^H(t)^* \ll p_A^M(t)^*, p_A^L(t)^*$.

(4)综合分析图 2 ~ 图 4,对防御者而言,在 $t\in[0,2]$ 内,应当以较高的概率 $p_D^H(t)^*\geqslant 0.76$ 选取强防御策略 D_H,面对突然爆发的高强度攻击可以最大程度的减少预期损失,因此 $p_D^H(t)^*$ 不断增加,在 $t=2$ 时刻达到峰值 0.89. 之后 $p_D^H(t)^*$ 逐渐降低,因为此时攻击者趋向采用较低强度的策略 A_M 和 A_L,防御者在考虑策略代价的情况下开始降低采用强防御策略的概率. 但是,为了保证防御效果,$p_D^H(t)^*$ 依然维持较高水平,在 $t\in[2,7]$ 内,$p_D^H(t)^*>0.67$. 在 $t=7$ 时刻之后,为尽快修复感染节点,避免后期损失,强防御策略的概率迅速提升,在 $t=10$ 时刻,$p_D^H(t)^*=0.91$.

不同状态网络节点的数量变化如图 5 所示.

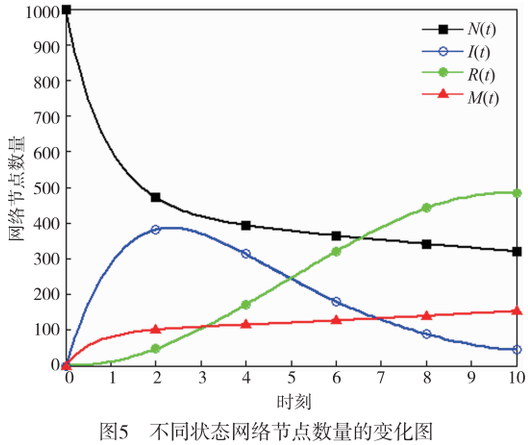

图5 不同状态网络节点数量的变化图

(5)在 $t\in[0,2]$ 时,由于攻击者的先发优势,一方面感染节点的数量迅速增加;另一方面受损节点的数量增幅较大;正常节点的数量极剧减少,$N(0)=1000$,$N(2)=464$,短时间内减少了 53.6%. 在 $t\in[2,3]$ 时,防御策略有效扼制了网络攻击,感染节点数量呈下降趋势. $t=3$ 时刻开始,强攻击策略的概率维持低水平,而强防御策略的概率保持高水平,因此修复节点的数量显著增长,受损节点的数量增长缓慢.

综合上述分析,提出以下建议:(1)防御者应在平时加大防御投入,提高防御能力,防范于未然,避免突然受到攻击时由于准备不足而遭受严重损失;(2)通过实时决策缩短防御决策时间和应急调整时间,实现对网络攻击的迅速、及时应对,避免更大损失;(3)合理使用主动防御措施,争取应急响应时间,避免由于反应不及而遭受严重损失.

5 结束语

本文对连续过程中的网络攻防行为进行分析研究,构建了攻防微分博弈模型,在此基础上,提出了鞍点策略的求解方法和最优防御策略选取算法. 通过仿真实验对本文提出模型和方法的有效性及合理性进行了验证,并基于实验数据分析对网络防御提出了针对性建议. 研究成果为连续、实时条件下的攻防对抗研究提供了有效的模型方法,并能够对防御策略的选取提供指导.

未来工作主要是改进网络攻防效能和博弈收益的计算方法,从多属性角度提升计算的精确性.

参考文献

[1] Gordon L, Loeb M. Budgeting process for information security expenditures[J]. Communications of the ACM, 2016, 49(10): 121 – 125.

[2] 王元卓,于建业,邱雯. 网络群体行为的演化博弈模型与分析方法[J]. 计算机学报,2015,38(2):282 – 300.
WANG Yuan-zhuo, YU Jian-ye, QIU Wen. Evolutionary game model and analysis methods for network group behavior[J]. Chinese Journal of Computers, 2015, 38(2): 282 – 300. (in Chinese)

[3] 姜伟,方滨兴,田志宏. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报,2013,32(4):818 – 827.
JIANG Wei, FANG Bing-xing. Defense strategies selection based on attack-defense game model[J]. Chinese Journal of Computers, 2013, 47(12): 818 – 827. (in Chinese)

[4] 余定坤,王晋东. 静态贝叶斯博弈主动防御策略选取方法[J]. 西安电子科技大学学报,2016,43(1):163 – 169.
YU Ding-kun, WANG Jin-dong. Active defense strategy selection based on static Bayesian game[J]. Journal of Xidian University, 2016, 43(1): 163 – 169. (in Chinese)

[5] WANG Yuan-zhuo, LIN Chuang, CHENG Xue-Qi, FANG Bing-xing. Evolutionary game model and analysis methods for network group behavior[J]. Journal of Computer Science and Technology, 2014, 38(2): 282 – 300.

[6] Wang Chun-lei, Miao Qing, Dai Yi-qi. Network survivability analysis based on stochastic game model[J]. Multimedia Information Networking and Security, 2015, 55(10): 199 – 204.

[7] 张恒巍,余定坤. 信号博弈网络安全威胁评估方法[J],西安电子科技大学学报,2016,43(3):137 – 143.

ZHANG Heng-wei, YU Ding-kun. Network security threat assessment based on signaling game[J]. Journal of Xidian University, 2016, 43(3): 137 – 143. (in Chinese)

[8] 张恒巍,王晋东,李涛. 基于攻防信号博弈模型的防御策略选取方法[J]. 通信学报,2016,37(5):32 – 43.
ZHANG Heng-wei, WANG Jin-dong, LI Tao. Defense policies selection method based on attack-defense signaling game model[J]. Journal on Communications, 2016, 37(5): 32 – 43. (in Chinese)

[9] SHEN S G, LI Y J, XU H Y. Signaling game based strategy of intrusion detection in wireless sensor networks[J]. Computers & Mathematics with Applications, 2015, 62(6): 2404 – 2416.

[10] Doraszel A. Preventing DDoS attacks in wireless sensor networks: a repeated game theory approach[J]. ACM Transactions on Information and System Security, 2015, 13(2): 145 – 153.

[11] 张恒巍,李涛. 基于多阶段攻防信号博弈的最优主动防御[J]. 电子学报,2017,45(2):431 – 439.
ZHANG Heng-wei, LI Tao. Optimal active defense based on multi-stage attack-defense signaling game[J]. Acta electronica Sinica, 2017, 45(2): 431 – 439. (in Chinese)

[12] 范红旗,王胜,付强. 离散时间二人随机微分对策问题信息模式的数学描述[J]. 电子学报,2015,43(2):1355 – 1361.
FAN Hong-qi, WANG Sheng, FU Qiang. Mathematical descriptionfor information pattern of stochastic differential games[J]. Acta Electronica Sinica, 2015, 42(2): 1355 – 1361. (in Chinese)

[13] Martin A Nowak. Evolutionary Dynamics: Exploring the Equations of Life[M]. Boston: Harvard University Press, 2013.

[14] David W K Yeung, Leon A Petrosyan. Differential Games Theory[M]. New York: Springer Press, 2014.

[15] Gordon L, Loeb M, Lucyshyn W, Richardson R. 2015 CSI/FBI computer crime and security survey[A]. Proceedings of the 2015 Computer Security Institute[C]. San Francisco, USA: IEEE Press, 2015. 48 – 64.

[16] Maleki H, Valizadeh M, Koch W. Scalable simulation framework on network[DB/OL]. http://www. ssfnet. org, 2012-11-08/2016-09-23.

[17] Moore D, Shannon C, Voelker GM. Internet quarantine: Requirements for containing self-propagating code[A]. Proceedings of the 22th International Conference of the IEEE Computer and Communications Societies[C]. Houston, USA: IEEE Press, 2015. 169 – 179.

作者简介

张恒巍　男,1978 年出生,河南洛阳人,博士,信息工程大学副教授,研究方向为网络安全与攻防对抗、信息安全风险评估.
E-mail: zhw11qd@126. com

李　涛(通信作者)　男,1992 年出生,甘肃甘谷人,信息工程大学博士研究生,研究方向为网络安全主动防御.
E-mail: 1527105421@qq. com

黄世锐　男,1994 年出生,广东汕头人,信息工程大学硕士研究生,研究方向为网络安全行为分析.
E-mail: hsrfzhac@qq. com